

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	
	)	
Shuzo FUJIOKA	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: July 10, 2003	)	Confirmation No.: Unassigned
	)	
For: INFORMATION SECURITY	)	
MICROCOMPUTER HAVING AN	)	
INFORMATION SECURITY	)	
FUNCTION AND AUTHENTICATING	)	
AN EXTERNAL DEVICE	)	

**CLAIM FOR CONVENTION PRIORITY**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

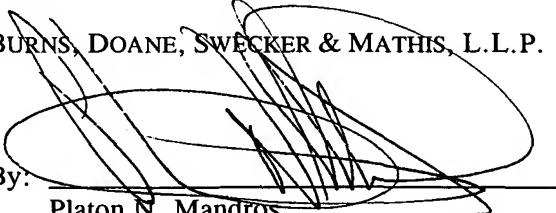
Japan Patent Application No. 2002-380316  
Filed: December 27, 2002

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: July 10, 2003

By:   
Platon N. Mandros  
Registration No. 22,124

P.O. Box 1404  
Alexandria, Virginia 22313-1404  
(703) 836-6620

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2002年12月27日

出 願 番 号  
Application Number:

特願2002-380316

[ST.10/C]:

[JP2002-380316]

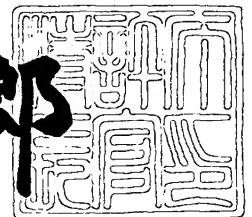
出 願 人  
Applicant(s):

三菱電機株式会社  
三菱電機システムエル・エス・アイ・デザイン株式会社

2003年 1月31日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3003031

【書類名】 特許願

【整理番号】 541256JP01

【提出日】 平成14年12月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14  
G06F 15/78

【発明者】

【住所又は居所】 兵庫県伊丹市中央3丁目1番17号 三菱電機システム  
エル・エス・アイ・デザイン株式会社内

【氏名】 藤岡 宗三

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【特許出願人】

【識別番号】 391024515

【氏名又は名称】 三菱電機システムエル・エス・アイ・デザイン株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100083703

【弁理士】

【氏名又は名称】 仲村 義平

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【選任した代理人】

【識別番号】 100098316

【弁理士】

【氏名又は名称】 野田 久登

【選任した代理人】

【識別番号】 100109162

【弁理士】

【氏名又は名称】 酒井 將行

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報セキュリティマイクロコンピュータ、そのプログラム開発装置およびそれらを含んだプログラム開発システム

【特許請求の範囲】

【請求項 1】 情報セキュリティ機能を有する情報セキュリティマイクロコンピュータであって、

情報の暗号化および復号を行なうための暗号手段と、

外部機器の認証を行なうための認証手段と、

前記情報セキュリティマイクロコンピュータの全体的な制御を行ない、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む、情報セキュリティマイクロコンピュータ。

【請求項 2】 前記プロセッサは、乱数を発生させて前記外部機器へ送信し、前記外部機器から受信した情報を復号し、該復号された値が前記乱数と一致するか否かを判定して前記外部機器の認証を行なう、請求項 1 記載の情報セキュリティマイクロコンピュータ。

【請求項 3】 前記プロセッサは、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータ全体の動作を停止させる、請求項 1 または 2 記載の情報セキュリティマイクロコンピュータ。

【請求項 4】 前記プロセッサは、前記認証手段によって認証が確認されなかった場合には、前記暗号手段の動作を停止させる、請求項 1 または 2 記載の情報セキュリティマイクロコンピュータ。

【請求項 5】 前記プロセッサは、前記認証手段によって認証が確認されなかった場合には、前記暗号手段による演算結果を正しく出力しないようにする、請求項 1 または 2 記載の情報セキュリティマイクロコンピュータ。

【請求項 6】 前記プロセッサは、デバッグモードおよび一般モードのいずれかで動作し、

前記情報セキュリティマイクロコンピュータはさらに、デバッグモードに固定するためのモードロック手段を含む、請求項 1 ～ 5 のいずれかに記載の情報セキ

ュリティマイクロコンピュータ。

【請求項 7】 情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、前記情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体とを含んだプログラム開発装置であって、

前記本体は、前記情報セキュリティマイクロコンピュータとの認証を行ない、コマンドを発行して前記情報セキュリティマイクロコンピュータを制御するための制御手段を含み、

前記情報セキュリティマイクロコンピュータは、前記本体との認証を行なうための認証手段と、

前記情報セキュリティマイクロコンピュータの全体的な制御を行ない、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む、プログラム開発装置。

【請求項 8】 情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、

前記情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体と、

前記本体を介して前記情報セキュリティマイクロコンピュータにコマンドを発行するコンピュータとを含み、

前記情報セキュリティマイクロコンピュータ、前記本体および前記コンピュータのうち、少なくともいずれか 2 つの間で認証を行なう、プログラム開発システム。

【請求項 9】 前記情報セキュリティマイクロコンピュータは、情報の暗号化および復号を行なうための暗号手段と、

前記本体または前記コンピュータの認証を行なうための認証手段と、

前記情報セキュリティマイクロコンピュータの全体的な制御を行ない、前記認証手段によって認証が確認されなかった場合には、前記情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む、請求項 8 記載のプログラム開発システム。

【請求項 1 0】 前記情報セキュリティマイクロコンピュータ、前記本体および前記コンピュータのうち、少なくともいずれか 2 つの間で行なわれる認証は、一定時間毎に繰返し行なわれる、請求項 8 または 9 記載のプログラム開発システム。

【請求項 1 1】 前記本体は、前記コンピュータとの認証を行ない、認証が確認されなかった場合には前記本体の少なくとも一部の機能が動作しないように制御する、請求項 8 ～ 1 0 のいずれかに記載のプログラム開発システム。

【請求項 1 2】 前記本体は、前記コンピュータとの認証を行なうと共に、前記情報セキュリティマイクロコンピュータとの認証を行ない、いずれかの認証が確認されなかった場合には前記情報セキュリティマイクロコンピュータまたは本体の少なくとも一部の機能が動作しないように制御を行なう、請求項 8 ～ 1 0 のいずれかに記載のプログラム開発システム。

【請求項 1 3】 前記コンピュータは、利用者からの認証情報を受けて前記情報セキュリティマイクロコンピュータに送信し、

前記情報セキュリティマイクロコンピュータは、前記コンピュータから受信した認証情報が予め保持する認証情報と一致するか否かを判定し、

前記コンピュータは、前記情報セキュリティマイクロコンピュータによって認証情報が一致しないと判定された場合には、前記本体の少なくとも一部の機能が動作しないように制御する、請求項 8 ～ 1 2 のいずれかに記載のプログラム開発システム。

【請求項 1 4】 前記コンピュータは、利用者による入力 that 一定時間以上なかった場合には、利用者に対して再度認証情報を入力させる、請求項 1 3 記載のプログラム開発システム。

【請求項 1 5】 前記プログラム開発システムはさらに、前記コンピュータと前記本体とを接続するネットワークを含み、

前記コンピュータは、前記本体にプログラムをダウンロードするときに、当該プログラムを暗号化して送信し、

前記本体は、前記コンピュータから受信した前記暗号化されたプログラムを復号して実行する、請求項 8 ～ 1 0 のいずれかに記載のプログラム開発システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ機能を搭載したマイクロコンピュータ（以下、情報セキュリティマイコンと略す。）に関し、特に、インサーキットエミュレータ（以下、ICEと略す。）に使用される情報セキュリティマイコン、そのプログラム開発装置およびそれらを含んだプログラム開発システムに関する。

【0002】

【従来の技術】

近年、ユーザの正当性の確認や情報の漏洩の防止などに情報セキュリティが広く用いられており、情報セキュリティ機能を搭載したマイコンの開発も進んでいる。このような情報セキュリティマイコンにおいても、一般のマイコンと同様にプログラム開発時にICEを用いてデバッグが行なわれる。

【0003】

ICE本体は、パーソナルコンピュータ（以下、PCと略す。）との接続に使用されるホストインタフェースや、ICE用マイコンとの接続に使用されるICEインタフェースを有しており、さらにICE全体の制御を行なう機能も有しているものもある。

【0004】

ICE本体は、PCからの命令によって、ICE用マイコンに対するプログラムの実行、ターゲットボードに搭載されたメモリの内容のダンプ、プログラムを1命令ずつ実行させるステップ実行、プログラムを所定の番地で停止させるブレークなどの機能を実現する。これに関連する技術として、特開2000-347942号公報に開示された発明がある。

【0005】

特開2000-347942号公報に開示された情報処理装置においては、ROM (Read Only Memory) に記憶された情報を外部に設けられたデバッグツールによる不正アクセスから保護するものであり、予め登録されたコードと外部から与えられたパスワードとを照合し、両者が一致した場合にはオンチップデバッグ

回路の機能を有効にするものである。

【0006】

【特許文献1】

特開2000-347942号公報

【0007】

【発明が解決しようとする課題】

上述したICEは、本来マイコンのプログラム開発に利用されるものであるが、悪用されるとリバースエンジニアリング、プログラムの解析、情報の改ざんなどが可能になるといった問題点があった。

【0008】

また、従来のICEは、接続の権限がない外部機器を接続しても動作するため、悪意を有する者がICEを利用して情報セキュリティマイコンを搭載したシステムを解析したり、情報セキュリティマイコンを偽造したりすることが可能になるといった問題点があった。

【0009】

また、ICE用マイコンは、プログラム開発の対象である情報セキュリティマイコンと同じ機能と、ICE本体からの制御を可能にするICEインタフェースとを有しており、情報セキュリティマイコンの代わりにICE用マイコンをシステムボードに載せることによって、システムの偽造に利用されたり、対象である情報セキュリティマイコンの解析に利用されたりするといった問題点があった。

【0010】

また、ICEに接続されるPCには、情報セキュリティマイコンが実行するプログラムなどのセキュリティ情報が格納されており、誰でもそのPCを利用できるとプログラムが盗まれるといった問題点があった。

【0011】

また、PCおよびICEをネットワークに接続したシステムにおいては、ICEを用いてプログラムをデバッグする場合、プログラムをPCからICEにダウンロードするため、その情報が傍受されてプログラムが盗用される可能性があるといった問題点があった。

## 【 0 0 1 2 】

さらには、上述した特開 2 0 0 0 - 3 4 7 9 4 2 号公報に開示された情報処理装置においては、予め登録されたコードと外部から与えられたパスワードとを照合し、両者が一致した場合にはオンチップデバッグ回路の機能を有効にして R O M に対する不正アクセスを防止するものであるが、パスワードを入力すれば接続の権限がない外部機器であっても R O M の内容を読み出すことができるため、セキュリティの強化を図ることができない。

## 【 0 0 1 3 】

本発明は、上記問題点を解決するためになされたものであり、その目的は、使用権限がない者が I C E 用マイコンとして利用することが不可能な情報セキュリティマイクロコンピュータを提供することである。

## 【 0 0 1 4 】

## 【課題を解決するための手段】

本発明のある局面に従えば、情報セキュリティ機能を有する情報セキュリティマイクロコンピュータであって、情報の暗号化および復号を行なうための暗号手段と、外部機器の認証を行なうための認証手段と、情報セキュリティマイクロコンピュータの全体的な制御を行ない、認証手段によって認証が確認されなかった場合には、情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む。

## 【 0 0 1 5 】

本発明の別の局面に従えば、情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体とを含んだプログラム開発装置であって、本体は、情報セキュリティマイクロコンピュータとの認証を行ない、コマンドを発行して情報セキュリティマイクロコンピュータを制御するための制御手段を含み、情報セキュリティマイクロコンピュータは、本体との認証を行なうための認証手段と、情報セキュリティマイクロコンピュータの全体的な制御を行ない、認証手段によって認証が確認されなかった場合には、情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるプロセッサとを含む。

## 【0016】

本発明のさらに別の局面に従えば、プログラム開発システムは、情報セキュリティ機能を有する情報セキュリティマイクロコンピュータと、情報セキュリティマイクロコンピュータを制御してプログラム開発を支援する本体と、本体を介して情報セキュリティマイクロコンピュータにコマンドを発行するコンピュータとを含み、情報セキュリティマイクロコンピュータ、本体およびコンピュータのうち、少なくともいずれか2つの間で認証を行なう。

## 【0017】

## 【発明の実施の形態】

## (第1の実施の形態)

図1は、本発明の第1の実施の形態におけるICE用マイコンの概略構成を示すブロック図である。このICE用マイコン1は、ICE用マイコン全体の制御を行なうCPU (Central Processing Unit) 11と、プログラムやデータを記憶するメモリ12と、認証データなどが格納される不揮発メモリ13と、外部機器との通信を行なう通信回路14と、ICE本体と通信を行なうICEインタフェース15と、所定のデータを認証データによって暗号化および復号を行ない、乱数を発生させる暗号回路16と、ICE本体との間の認証を行なう認証用プログラム17とを含む。

## 【0018】

暗号回路16は、不揮発メモリ13に格納された認証データを参照して暗号化および復号を行なうプログラムを、CPU11が実行することによって実現される。また、CPU11が認証用プログラム17を実行することによって、ICE本体の認証が行なわれる。この認証用プログラム17は、メモリ12に格納されているもよい。

## 【0019】

図2は、ICE用マイコン1とICE本体との間の認証を説明するための図である。図2においては、認証の一例としてチャレンジ&レスポンス方式の認証を示しており、共通鍵暗号方式を利用した場合を示している。ICE用マイコン1とICE本体とに、予め同じ暗号鍵が認証データとして格納されているものとす

る。なお、共通鍵暗号方式ではなく、公開鍵暗号方式を用いてもよい。

【 0 0 2 0 】

まず、ICE用マイコン1（認証する側）内のCPU11は、認証用プログラム17を実行することによって乱数を発生させ、生成した乱数をICEインタフェース15を介してICE本体（認証される側）へ送信する。

【 0 0 2 1 】

ICE本体は、ICE用マイコン1から乱数を受信し、この乱数を予め格納している認証データを用いて暗号化する。そして、ICE本体は、この暗号化した乱数をICE用マイコン1へ送信する。

【 0 0 2 2 】

ICE用マイコン1は、ICE本体から暗号化された乱数を受信し、不揮発メモリ13に予め格納される認証データを用いてそれを復号する。そして、復号された値が自身が生成した乱数と一致する場合には、ICE本体の認証が確認されたものとする。また、復号された値が自身が生成した乱数と一致しない場合には、ICE本体の認証が確認されなかったものとする。

【 0 0 2 3 】

図3は、本発明の第1の実施の形態におけるICE用マイコン1を用いたプログラム開発システムの一例を示す図である。このプログラム開発システムは、ICE2と、ICE2に接続されるPC3と、ターゲットボード4とを含む。また、ICE2は、ICE本体21と、ICE用マイコン1が搭載されるPOD22とを含む。POD22は、ターゲットボード4に接続される。

【 0 0 2 4 】

PC3は、ICE2に対して命令を送信することによって、ICE用マイコン1に対するプログラムの実行、ターゲットボード4に搭載されたメモリの内容のダンプ、プログラムを1命令ずつ実行させるステップ実行、プログラムを所定の番地で停止させるブレークなどの機能を実現する。

【 0 0 2 5 】

図4は、ICE2の機能的構成を示すブロック図である。ICE2は、ICE2の全体的な制御を行なうICE制御部（ICE本体）21と、ICE用マイコ

ン 1 が搭載される P O D 2 2 とを含む。

【 0 0 2 6 】

I C E 制御部 2 1 は、予め認証データを保持しており、I C E 用マイコン 1 から乱数を受信すると、認証データを用いて乱数を暗号化して I C E 用マイコン 1 へ送信する。また、I C E 制御部 2 1 は、P C 3 から命令を受信すると、その命令を P O D 2 2 に搭載された I C E 用マイコン 1 へ送信する。

【 0 0 2 7 】

図 5 は、本発明の第 1 の実施の形態における I C E 用マイコン 1 を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。まず、P O D 2 2 に搭載された I C E 用マイコン 1 が動作を開始すると、C P U 1 1 は乱数を発生させ ( S 1 1 ) 、その乱数を I C E インタフェース 1 5 を介して I C E 本体 2 1 へ送信する ( S 1 2 ) 。

【 0 0 2 8 】

I C E 本体 2 1 は、I C E 用マイコン 1 から乱数を受信すると ( S 1 3 ) 、予め保持している認証データを暗号鍵として用い、受信した乱数を暗号化する。そして、I C E 本体 2 1 は、暗号化した乱数を I C E 用マイコン 1 へ送信する ( S 1 4 ) 。

【 0 0 2 9 】

I C E 用マイコン 1 は、I C E 本体 2 1 から暗号化された乱数を受信すると ( S 1 5 ) 、予め不揮発メモリ 1 3 に保持している認証データを復号鍵として用い、受信した暗号化された乱数を復号する ( S 1 6 ) 。そして、I C E 用マイコン 1 は、復号した値と自身が生成した乱数とを比較する ( S 1 7 ) 。

【 0 0 3 0 】

復号した値と自身が生成した乱数とが一致しない場合には ( S 1 8 , Y e s ) 、I C E 用マイコン 1 全体の動作を停止させる ( S 1 9 ) 。また、復号した値と自身が生成した乱数とが一致する場合には ( S 1 8 , N o ) 、I C E 機能の動作を開始する ( S 2 0 ) 。

【 0 0 3 1 】

I C E 本体 2 1 が I C E 用マイコン 1 に対してコマンドを送信すると ( S 2 1

）、ICE用マイコン1はコマンドを受信し（S22）、当該コマンドを実行する（S23）。そして、ICE用マイコン1はコマンドの実行結果をICE本体21へ送信する（S24）。ICE本体21は、ICE用マイコン1からコマンドの実行結果を受信すると（S25）、その実行結果をPC3へ送信して、PC3から次の命令を受信するまで待機する。

【0032】

以上の説明においては、ICE用マイコン1がICE本体21の認証を行なうものであったが、ICE本体21がICE用マイコン1の認証を行うようにすれば両方の認証が行なえるため、さらにセキュリティを高めることが可能となる。

【0033】

以上説明したように、本実施の形態におけるICE用マイコン1によれば、ICE本体21の認証を行ない、認証が確認された場合にはICE機能の動作を行ない、認証が確認されなかった場合にはICE用マイコン1の動作を停止するようにしたので、悪意のある者が別のシステムでそのICE用マイコンを利用することができなくなり、セキュリティを向上させることが可能となった。

【0034】

（第2の実施の形態）

本発明の第1の実施の形態におけるICE用マイコン1においては、認証が確認されなかった場合にはICE用マイコン1の動作を全て停止させるものであったが、第2の実施の形態におけるICE用マイコン1は認証が確認されなかった場合にはICE用マイコン1内の暗号回路16の動作のみを停止させるものである。

【0035】

本発明の第2の実施の形態におけるICE用マイコンは、図1に示す第1の実施の形態におけるICE用マイコンと比較して、ICE本体21の認証が確認されなかった場合には暗号回路16の動作のみが停止される点を除いて同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【0036】

図6は、本発明の第2の実施の形態におけるICE用マイコン1を用いたプロ

グラム開発システムの処理手順を説明するためのフローチャートである。図 5 に示す第 1 の実施の形態におけるプログラム開発システムの処理手順と比較して、ステップ S 1 9 の処理のみが異なる。したがって、重複する処理手順の詳細な説明は省略する。なお、本実施の形態におけるステップ S 1 9 の参照符号を S 1 9' として説明する。

【 0 0 3 7 】

ステップ S 1 8 において、復号した値と自身が生成した乱数とが一致しない場合には ( S 1 8 , Y e s ) 、 I C E 用マイコン 1 内の暗号回路 1 6 の動作のみを停止させる ( S 1 9' ) 。また、復号した値と自身が生成した乱数とが一致する場合には ( S 1 8 , N o ) 、 I C E 機能の動作を開始する ( S 2 0 ) 。

【 0 0 3 8 】

一般に、セキュリティに関するデバッグは、暗号回路 1 6 を利用したプログラムに集中するため、セキュリティに関するプログラムのデバッグを行なう者のみに暗号回路 1 6 の使用を認め、それ以外の者には暗号回路 1 6 の使用を認めないようにすることができる。たとえば、P C の起動時に I C E 2 に利用者認証を要求し、I C E 本体 2 1 が I C E 用マイコン 1 との認証を行なうようにする。そして、認証が確認されれば、暗号回路 1 6 を含んだ I C E 用マイコン 1 全体の動作を認め、認証が確認されなければ、暗号回路 1 6 の動作のみを停止してそれ以外の動作を認める。

【 0 0 3 9 】

以上説明したように、本実施の形態における I C E 用マイコン 1 によれば、I C E 本体 2 1 の認証を行ない、認証が確認された場合には I C E 機能の動作を行ない、認証が確認されなかった場合には I C E 用マイコン 1 内の暗号回路 1 6 の動作のみを停止するようにしたので、利用権限を有する開発者のみが暗号回路 1 6 を利用したデバッグを行なえ、利用権限を有しない開発者には暗号回路 1 6 を利用しないデバッグのみを行えるようにするといった、役割分担に応じたプログラム開発が可能になった。

【 0 0 4 0 】

( 第 3 の実施の形態 )

本発明の第 1 の実施の形態における I C E 用マイコン 1 においては、認証が確認されなかった場合には I C E 用マイコン 1 の動作を全て停止させるものであったが、第 3 の実施の形態における I C E 用マイコン 1 は認証が確認されなかった場合には I C E 用マイコン 1 内の暗号回路 1 6 が正しい演算結果を出力しないようにしたものである。

【 0 0 4 1 】

本発明の第 3 の実施の形態における I C E 用マイコンは、図 1 に示す第 1 の実施の形態における I C E 用マイコンと比較して、I C E 本体 2 1 の認証が確認されなかった場合には暗号回路 1 6 が正しい演算結果を出力しない点を除いて同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【 0 0 4 2 】

図 7 は、本発明の第 3 の実施の形態における I C E 用マイコン 1 を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。図 5 に示す第 1 の実施の形態におけるプログラム開発システムの処理手順と比較して、ステップ S 1 9 の処理のみが異なる。したがって、重複する処理手順の詳細な説明は省略する。なお、本実施の形態におけるステップ S 1 9 の参照符号を S 1 9 ” として説明する。

【 0 0 4 3 】

ステップ S 1 8 において、復号した値と自身が生成した乱数とが一致しない場合には ( S 1 8 , Y e s ) 、 I C E 用マイコン 1 内の暗号回路 1 6 が正しい演算結果を出力しない ( S 1 9 ” ) 。また、復号した値と自身が生成した乱数とが一致する場合には ( S 1 8 , N o ) 、 I C E 機能の動作を開始する ( S 2 0 ) 。なお、復号した値と自身が生成した乱数とが一致しない場合には、演算結果を全く出力しないようにしてもよい。

【 0 0 4 4 】

一般に、セキュリティに関係するデバッグは、暗号回路 1 6 を利用したプログラムに集中するため、セキュリティに関するプログラムのデバッグを行なう者のみに暗号回路 1 6 の使用を認め、それ以外の者には暗号回路 1 6 の使用を認めるがセキュリティ情報の確認を行なえないようにすることができる。たとえば、P

Cの起動時にICE 2に利用者認証を要求し、ICE本体21がICE用マイコン1との認証を行なうようにする。そして、認証が確認されれば、暗号回路16を含んだICE用マイコン1全体の動作を認め、認証が確認されなければ、暗号回路16が正しい演算結果を出力しないように動作し、それ以外のICE用マイコン1の動作を認める。

【0045】

以上説明したように、本実施の形態におけるICE用マイコン1によれば、ICE本体21の認証を行ない、認証が確認された場合にはICE機能の動作を行ない、認証が確認されなかった場合にはICE用マイコン1内の暗号回路16が正しい演算結果を出力しないようにしたので、利用権限を有する開発者のみが暗号回路16を利用したデバッグを行なえ、利用権限を有しない開発者は暗号回路16の機能的な検証は行なえるが、セキュリティ情報の確認を行なうことができないといった、役割分担に応じたプログラム開発が可能になった。

【0046】

(第4の実施の形態)

本発明の第4の実施の形態におけるプログラム開発システムの概略構成は、図3に示す第1の実施の形態におけるプログラム開発システムの概略構成と同様である。また、本発明の第4の実施の形態におけるICE 2の機能的構成は、図4に示す第1の実施の形態におけるICE 2の機能的構成と同様である。したがって、重複する構成および機能の詳細な説明は繰返さない。

【0047】

図8は、本発明の第4の実施の形態におけるICE本体21の機能的構成を示すブロック図である。ICE本体21は、ICE本体21の全体的な制御を行なうICE制御部211と、認証用プログラム212と、認証データ213とを含む。

【0048】

ICE制御部211は、PC3との間で通信を行なうホストインタフェースと、ICE用マイコン1との間で通信を行なうICEインタフェースとを有している。ICE制御部211は、ホストインタフェースを介してPC3からコマンド

を受信すると、ICE用マイコン1にそのコマンドを送信する。ICE用制御部211は、ICE用マイコン1からそのコマンドの実行結果を受信すると、実行結果をPC3へ送信する。このようにして、PC3はICEマイコン1の動作を制御することが可能になる。

【0049】

ICE本体21は、ICE用マイコン1に格納される認証データと同じ認証データ213を有しており、認証用プログラム212は、認証データ213を用いてICE用マイコン1と同様の認証を行なう。ICE用マイコン1の認証が確認されなかった場合のICE用マイコン1の動作は、図5～図7を用いて説明した第1～第3の実施の形態におけるICE用マイコン1の動作と同様である。

【0050】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ICE本体21がICE用マイコン1の認証を行なうようにしたので、認証機能を持たないICE本体21はICE用マイコン1を用いてデバッグ等を行なえなくなり、セキュリティを向上させることが可能となった。

【0051】

(第5の実施の形態)

図9は、本発明の第5の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、PC3と、ICE本体21と、POD22と、ターゲットボード4とを含む。PC3は、認証用プログラムおよび認証データを格納しており、ICE用マイコン1がPC3の認証を行なう。PC3の認証が確認されなかった場合のICE用マイコン1の動作は、図5～図7を用いて説明した第1～第3の実施の形態におけるICE用マイコン1の動作と同様である。

【0052】

図10は、本発明の第5の実施の形態におけるプログラム開発システムの概略構成の他の一例を示すブロック図である。このプログラム開発システムは、PC3と、POD22と、ターゲットボード4とを含む。PC3は、ICE本体21が有する機能を有しており、PC3が直接POD22内のICE用マイコン1と

通信を行なうことにより、ICE用マイコン1がPC3の認証を行なう。

【0053】

以上の説明においては、ICE用マイコン1がPC3の認証を行なうものであったが、PC3がICE用マイコン1の認証を行うようにすれば両方の認証が行なえるため、さらにセキュリティを高めることが可能となる。

【0054】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ICE用マイコン1とPC3との間で認証を行なうようにしたので、ICE用マイコン1を利用する権限のないPC3はICE用マイコン1を動作させることができないため、セキュリティを向上させることが可能となった。また、PC3以外の計測機器を接続した場合でも、ICE用マイコン1との間の認証が行なわれないので、ICE用マイコン1の解析を防止することが可能となった。

【0055】

（第6の実施の形態）

図11は、本発明の第6の実施の形態におけるプログラム開発システムの概略構成を示すブロック図である。このプログラム開発システムは、PC3と、ICE本体21と、POD22と、ターゲットボード4とを含む。PC3は、認証用プログラムおよび認証データを格納している。また、ICE本体21も認証用プログラムおよび認証データを格納しており、ICE本体21がPC3の認証を行なう。PC3の認証が確認されなかった場合のICE用マイコン1の動作は、図5～図7を用いて説明した第1～第3の実施の形態におけるICE用マイコン1の動作と同様である。

【0056】

以上の説明においては、ICE本体21がPC3の認証を行なうものであったが、PC3がICE本体21の認証を行うようにすれば両方の認証が行なえるため、さらにセキュリティを高めることが可能となる。

【0057】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ICE本体21とPC3との間で認証を行なうようにしたので、ICE本体2

1 を利用する権限のない PC 3 は ICE 用マイコン 1 を動作させることができないため、セキュリティを向上させることが可能となった。また、PC 3 以外の計測機器を接続した場合でも、ICE 本体 21 との間の認証が行なわれないので、ICE 用マイコン 1 の解析を防止することが可能となった。

【0058】

（第 7 の実施の形態）

図 12 は、本発明の第 7 の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、PC 3 と、ICE 本体 21 と、POD 22 と、ターゲットボード 4 とを含む。PC 3 は、認証用プログラムおよび認証データを格納している。また、ICE 本体 21 も認証用プログラムおよび認証データを格納している。

【0059】

ICE 用マイコン 1 と ICE 本体 21 との間で認証が行なわれると共に、ICE 本体 21 と PC 3 との間でも認証が行なわれる。ICE 用マイコン 1 と ICE 本体 21 との間の認証、および ICE 本体 21 と PC 3 との間の認証のいずれか、または両方の認証が確認されなかった場合の ICE 用マイコン 1 の動作は、図 5 ～図 7 を用いて説明した第 1 ～第 3 の実施の形態における ICE 用マイコン 1 の動作と同様である。

【0060】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ICE 用マイコン 1 と ICE 本体 21 との間、および ICE 本体 21 と PC 3 との間で認証を行なうようにしたので、ICE 用マイコン 1 を利用する権限のない ICE 本体 21 または PC 3 は ICE 用マイコン 1 を動作させることができないため、さらにセキュリティを向上させることが可能となった。

【0061】

（第 8 の実施の形態）

図 13 は、本発明の第 8 の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、PC 3 と、ICE 本体 21 と、POD 22 と、ターゲットボード 4 とを含む。PC 3 は、

利用者によるパスワードの入力を受け、そのパスワードをICE用マイコン1へ送信する。ICE用マイコン1は、PC3から受信したパスワードと予め格納しているパスワードとを比較し、その比較結果をPC3へ送信する。

【0062】

図14は、本発明の第8の実施の形態におけるプログラム開発システムの処理手順を説明するためのフローチャートである。まず、利用者がPC3にパスワードを入力すると(S31)、そのパスワードはICE本体21を介してICE用マイコン1へ送信される。

【0063】

ICE用マイコン1は、PC3から受信したパスワードと、予め格納しているパスワードとを比較する(S32)。パスワードが一致しなければ(S32, No)、ICE用マイコン1はPC3へパスワードが一致しなかったことを通知する(S33)。また、パスワードが一致すれば(S32, Yes)、ICE用マイコン1はPC3へパスワードが一致したことを通知する(S35)。

【0064】

PC3は、ICE用マイコン1からパスワードが一致しなかったことを示す通知を受けると、ICE2を制御するプログラムを停止させるか、ICE2の利用制限を行なう(S34)。また、PC3は、ICE用マイコン1からパスワードが一致したことを示す通知を受けると、PC3とICE本体21との認証を開始するか、ICE本体21とICE用マイコン1との認証を行なうよう指示する(S36)。

【0065】

PC3とICE本体21との認証、またはICE本体21とICE用マイコン1との認証が確認されれば(S37, No)、ICE2の起動を開始する(S38)。また、PC3とICE本体21との認証、またはICE本体21とICE用マイコン1との認証が確認されなければ(S37, Yes)、ICE2またはICE用マイコン1の動作を停止させるか、ICE2またはICE用マイコン1の動作の制限を行なう(S39)。

【0066】

また、PC 3 は、利用者による PC 3 の操作が一定時間なかった場合には、画面をロックするようにしてもよい。この場合、利用者が再度パスワードを入力することにより、画面のロックが解除される。このようにして、利用権限を有する者がいない間に、利用権限を有しない者が ICE 2 を利用してプログラムのデバッグや解析を行なうことを防止することができる。

【 0 0 6 7 】

また、パスワードと ID とを用いて利用者を管理するようにすれば、利用者に役割分担に応じた利用権限を与えることができる。たとえば、利用者によって入力された ID によって、ICE 用マイコン 1 が第 1 ～第 3 の実施の形態において説明した動作制限のいずれかを選択して実行するようにすれば、ID によってデバッグ可能なレベルを利用者毎に設定することができる。

【 0 0 6 8 】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、ICE 用マイコン 1 が、PC 3 から入力されたパスワードと予め保持するパスワードとを比較し、その比較結果に応じて ICE 用マイコン 1 または ICE 2 の動作を制限するようにしたので、セキュリティを向上させることが可能になると共に、利用者の利便性を向上させることが可能となった。

【 0 0 6 9 】

（第 9 の実施の形態）

本発明の第 9 の実施の形態におけるプログラム開発システムは、第 4 ～第 8 の実施の形態におけるプログラム開発システムと比較して、一定時間毎に認証を行う点を除いて同様である。したがって、重複する構成および機能の詳細な説明は繰返さない。

【 0 0 7 0 】

たとえば、第 4 の実施の形態におけるプログラム開発システムにおいて、ICE 用マイコン 1 と ICE 本体 2 1 との認証が確認された後、ICE 本体 2 1 が別の装置に摩り替えられた場合でも ICE 用マイコン 1 はそのまま動作を続けるので、利用権限のない者であっても ICE 2 を用いたプログラムのデバッグや解析が可能になる。これを防止するために、ICE 用マイコン 1 および ICE 本体 2

1 は一定時間毎に認証を行なうものである。

【 0 0 7 1 】

また、送受信されるコマンドやレスポンスに署名データを付加するようにすれば、装置の摩り替えを防止することができる。この場合、署名データの生成方法として、通信データを圧縮した後認証データで暗号化を行なえばよい。通信データの圧縮には、たとえばハッシュ関数などが利用できる。また、通信データを圧縮せずにそのまま暗号化してもよい。

【 0 0 7 2 】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、一定時間毎に再認証を行なうようにしたので、装置の摩り替えを防止することが可能となった。

【 0 0 7 3 】

(第 1 0 の実施の形態)

図 1 5 は、本発明の第 1 0 の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。このプログラム開発システムは、PC 3 と、ネットワーク 5 を介して PC 3 に接続される ICE 本体 2 1 と、POD 2 2 と、ターゲットボード 4 とを含む。

【 0 0 7 4 】

ICE 本体 2 1 を用いてプログラムをデバッグする場合、PC 3 から ICE 本体 2 1 にプログラムをダウンロードする必要がある。情報セキュリティマイコンのプログラムは機密性が高いため、ICE 本体 2 1 にダウンロードするプログラムが外部に漏れると、情報セキュリティマイコンを搭載したシステムの偽造などに用いられることが想定される。

【 0 0 7 5 】

PC 3 と ICE 本体 2 1 とが 1 対 1 で接続される場合はプログラムが傍受される危険性は少ないが、PC 3 と ICE 本体 2 1 とが LAN (Local Area Network) などのネットワーク 5 によって接続される場合にはプログラムが傍受される危険性が高くなる。これを防止するために、本実施の形態においては通信データを暗号化するものである。

## 【 0 0 7 6 】

たとえば、PC 3 と ICE 本体 2 1 との認証を行なう際に使用された認証データおよび暗号機能を用いて通信データ（プログラム）を暗号化し、ICE 本体 2 1 にダウンロードする。そして、ICE 本体 2 1 は、同じ認証データを用いて復号を行なってプログラムをメモリ 1 2 に格納する。また、通信用として認証用と別の認証データ（暗号鍵）および暗号機能を用いるようにしてもよい。

## 【 0 0 7 7 】

以上説明したように、本実施の形態におけるプログラム開発システムによれば、PC 3 が通信データを暗号化して ICE 本体 2 1 にダウンロードするようにしたので、ネットワークを介して通信データが傍受される危険性を少なくすることが可能となった。

## 【 0 0 7 8 】

（第 1 1 の実施の形態）

第 1 ～ 第 3 の実施の形態において説明した ICE 用マイコン 1 は、システムなどに組込まれる一般の情報セキュリティマイコンとして使用できる場合がある。

## 【 0 0 7 9 】

図 1 6 は、ICE モード（デバッグモード）と一般モードとを切替えて動作する ICE 用マイコンの構成例を示す図である。図 1 6 の上図に示すように、ICE モードで動作する場合には、ICE インタフェース 1 5 および ICE 機能プログラム（認証プログラム、認証データを含む。）1 8 が動作するように制御される。なお、ICE 機能プログラム 1 8 は、マスク ROM（Read Only Memory）、OTPROM（One Try Programmable ROM）などに格納される。

## 【 0 0 8 0 】

また、図 1 6 の下図に示すように、一般モードで動作する場合には、ICE インタフェース 1 5 および ICE 機能プログラム 1 8 が動作しないように制御される。なお、図 1 6 の上図が実際の ICE 用マイコンの構成であり、図 1 6 の下図が一般モードのときに設定される仮想上の構成である。

## 【 0 0 8 1 】

このように ICE 用マイコン 1 がどちらにも使用できる場合には、ICE モー

ドと一般モードとを有しており、モードを切替えて使用されることが多い。すなわち、ICEモードで動作するプログラムを削除すれば、一般の情報セキュリティマイコンとして使用できるため、情報セキュリティマイコンの偽造に使用される危険性がある。

## 【0082】

本実施の形態においては、ICEモードで動作するプログラムを削除できない構造にするか、ICEモードに固定して一般モードにならないようにすることによって、ICE用マイコン1が一般の情報セキュリティマイコンとして使用できないようにするものである。

## 【0083】

図17は、本発明の第11の実施の形態におけるICE用マイコンのモードロック回路の一例を示す図である。このモードロック回路は、OR回路31と、ヒューズ32とを含む。一般の情報セキュリティマイコンとして出荷する場合には、ヒューズ32をそのままにする。これによって、OR回路31は、モード切替え信号をそのまま出力するようになる。また、一般モードに固定されるようにしてもよい。

## 【0084】

ICE用マイコン1として出荷する場合には、ヒューズ32を切る。これによって、OR回路31は、モード切替え信号にかかわらずハイレベルを出力して、ICEモードに固定される。すなわち、一般の情報セキュリティマイコンとして使用できなくなる。

## 【0085】

図18は、本実施の形態におけるICE用マイコンのモードロック回路の他の一例を示す図である。このモードロック回路は、OR回路41と、ロックコード検出回路42とを含む。ロックコード検出回路42は、不揮発メモリ13の所定アドレスに書込まれているデータを読み出し、そのデータがロックコードと一致する場合にはハイレベルを出力する。また、そのデータがロックコードと一致しない場合にはロウレベルを出力する。

## 【0086】

一般の情報セキュリティマイコンとして出荷する場合には、不揮発メモリ 13 の所定アドレスにロックコード以外のデータを書込む。これによって、OR回路 41 は、モード切替え信号をそのまま出力するようになる。また、一般モードに固定されるようにしてもよい。

【0087】

ICE用マイコン 1 として出荷する場合には、不揮発メモリ 13 の所定アドレスにロックコードを書込む。これによって、OR回路 41 は、モード切替え信号にかかわらずハイレベルを出力して、ICEモードに固定される。すなわち、一般の情報セキュリティマイコンとして使用できなくなる。

【0088】

以上説明したように、本実施の形態におけるICE用マイコン 1 によれば、モードロック回路によってモードをICEモードに固定できるようにしたので、ICE用マイコン 1 を一般の情報セキュリティマイコンとして使用できなくなり、情報セキュリティマイコンの偽造に使用される危険性を少なくすることが可能となった。

【0089】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0090】

【発明の効果】

本発明のある局面によれば、認証手段によって外部機器の認証が確認されなかった場合には、プロセッサが情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるので、使用権限がない者が情報セキュリティマイクロコンピュータをICE用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となった。

【0091】

本発明の別の局面によれば、本体と情報セキュリティマイクロコンピュータと

の間で認証を行ない、認証が確認されなかった場合には、情報セキュリティマイクロコンピュータの少なくとも一部の機能を停止させるので、使用権限がない本体が情報セキュリティマイクロコンピュータをICE用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となった。

【0092】

本発明のさらに別の局面によれば、情報セキュリティマイクロコンピュータ、本体およびコンピュータのうち、少なくともいずれか2つの間で認証を行なうので、使用権限がない本体またはコンピュータが情報セキュリティマイクロコンピュータをICE用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となった。

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態におけるICE用マイコンの概略構成を示すブロック図である。

【図2】 ICE用マイコン1とICE本体との間の認証を説明するための図である。

【図3】 本発明の第1の実施の形態におけるICE用マイコン1を用いたプログラム開発システムの一例を示す図である。

【図4】 ICE2の機能的構成を示すブロック図である。

【図5】 本発明の第1の実施の形態におけるICE用マイコン1を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。

【図6】 本発明の第2の実施の形態におけるICE用マイコン1を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。

【図7】 本発明の第3の実施の形態におけるICE用マイコン1を用いたプログラム開発システムの処理手順を説明するためのフローチャートである。

【図8】 本発明の第4の実施の形態におけるICE本体21の機能的構成を示すブロック図である。

【図9】 本発明の第5の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図10】 本発明の第5の実施の形態におけるプログラム開発システムの

概略構成の他の一例を示すブロック図である。

【図 1 1】 本発明の第 6 の実施の形態におけるプログラム開発システムの概略構成を示すブロック図である。

【図 1 2】 本発明の第 7 の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図 1 3】 本発明の第 8 の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図 1 4】 本発明の第 8 の実施の形態におけるプログラム開発システムの処理手順を説明するためのフローチャートである。

【図 1 5】 本発明の第 1 0 の実施の形態におけるプログラム開発システムの概略構成の一例を示すブロック図である。

【図 1 6】 I C E モードと一般モードとを切替えて動作する I C E 用マイコンの構成例を示す図である。

【図 1 7】 本発明の第 1 1 の実施の形態における I C E 用マイコンのモードロック回路の一例を示す図である。

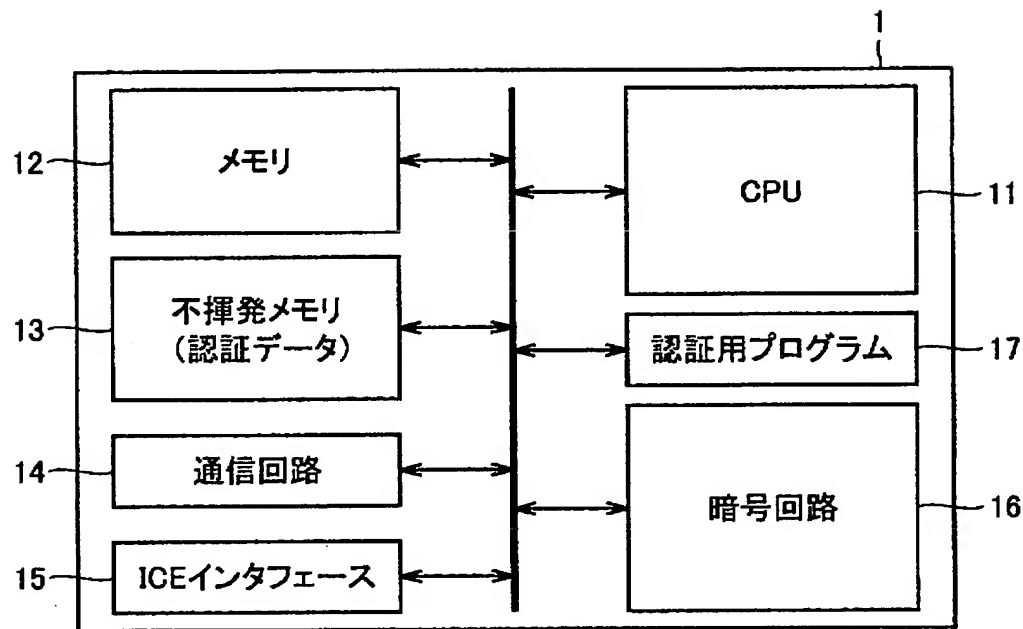
【図 1 8】 本発明の第 1 1 の実施の形態における I C E 用マイコンのモードロック回路の他の一例を示す図である。

【符号の説明】

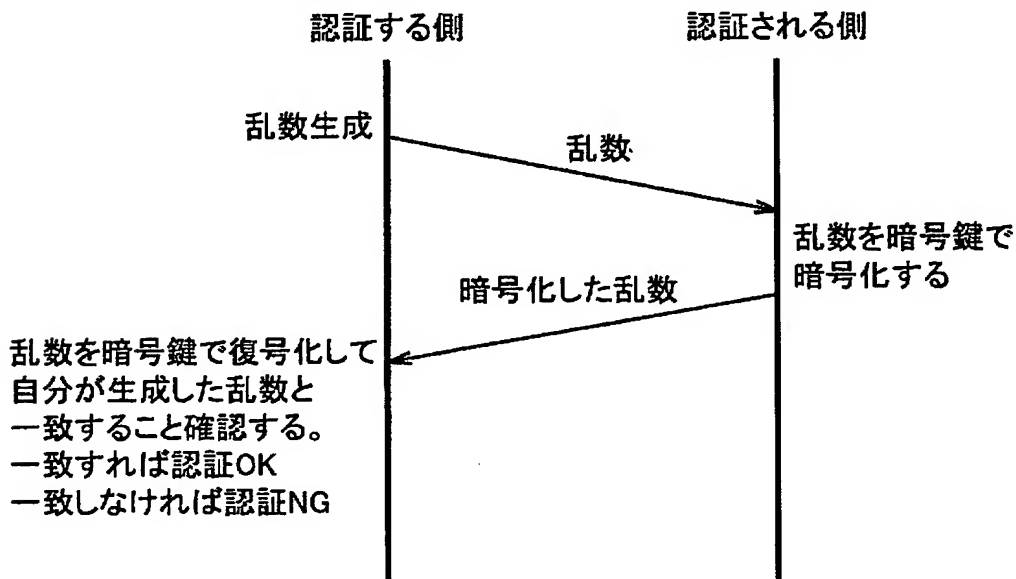
1 I C E 用マイコン、2 I C E、3 P C、4 ターゲットボード、5 ネットワーク、1 1 C P U、1 2 メモリ、1 3 不揮発メモリ、1 4 通信回路、1 5 I C E インタフェース、1 6 暗号回路、1 7、2 1 2 認証用プログラム、1 8 I C E 機能プログラム、2 1 I C E 本体、2 2 P O D、3 1、4 1 O R 回路、3 2 ヒューズ、4 2 ロックコード検出回路、2 1 1 I C E 制御部、2 1 3 認証データ。

【書類名】 図面

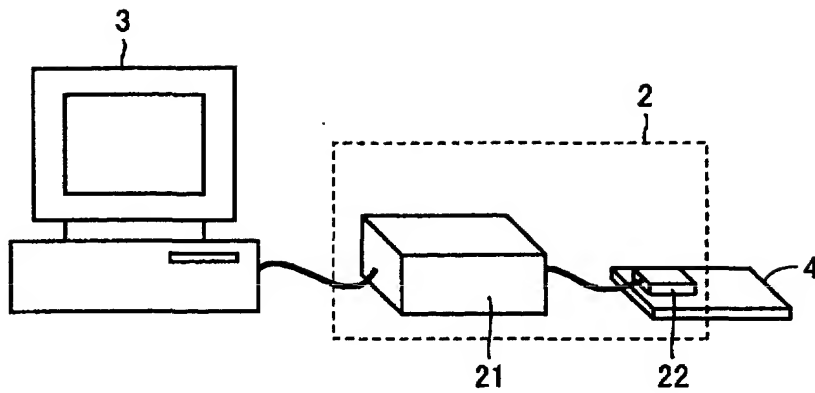
【図 1】



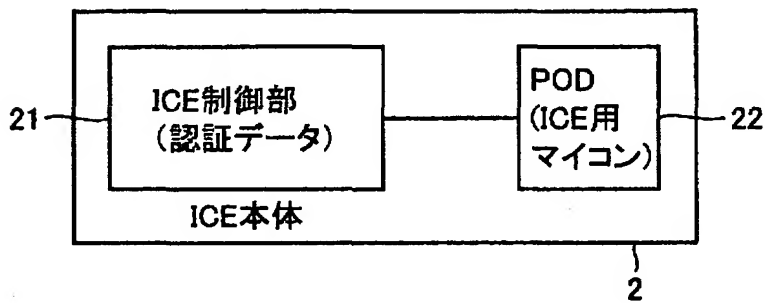
【図 2】



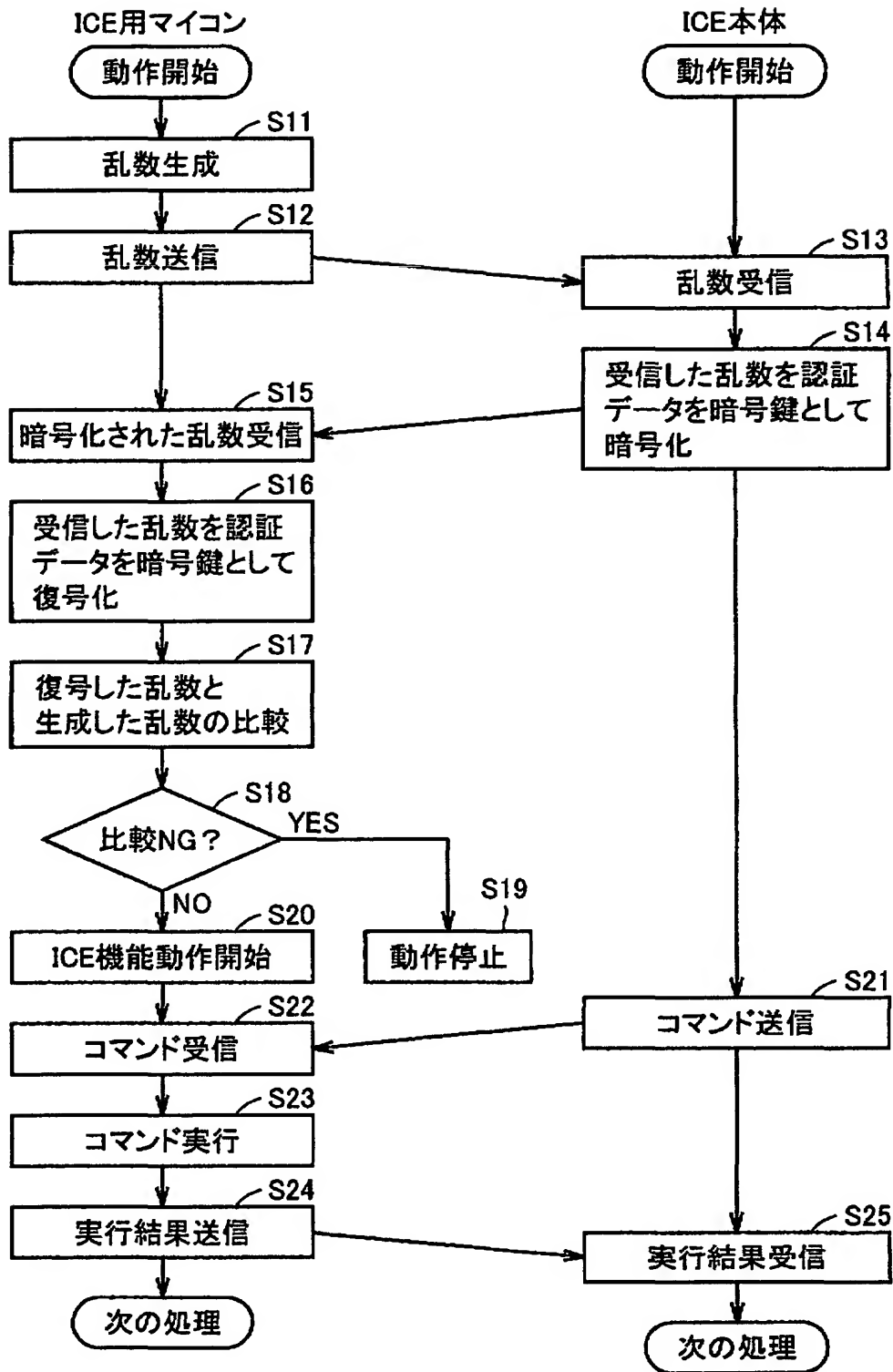
【図 3】



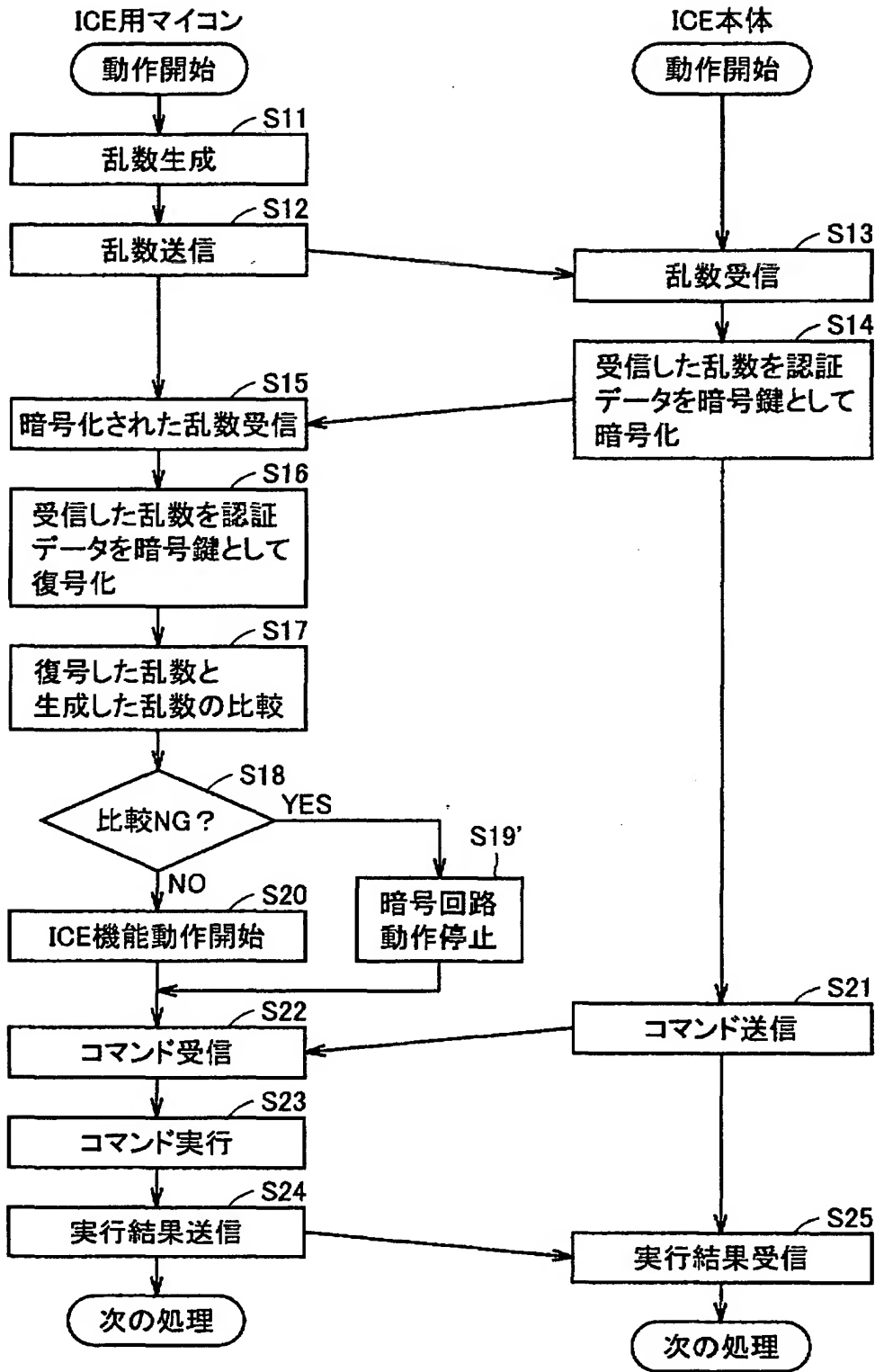
【図 4】



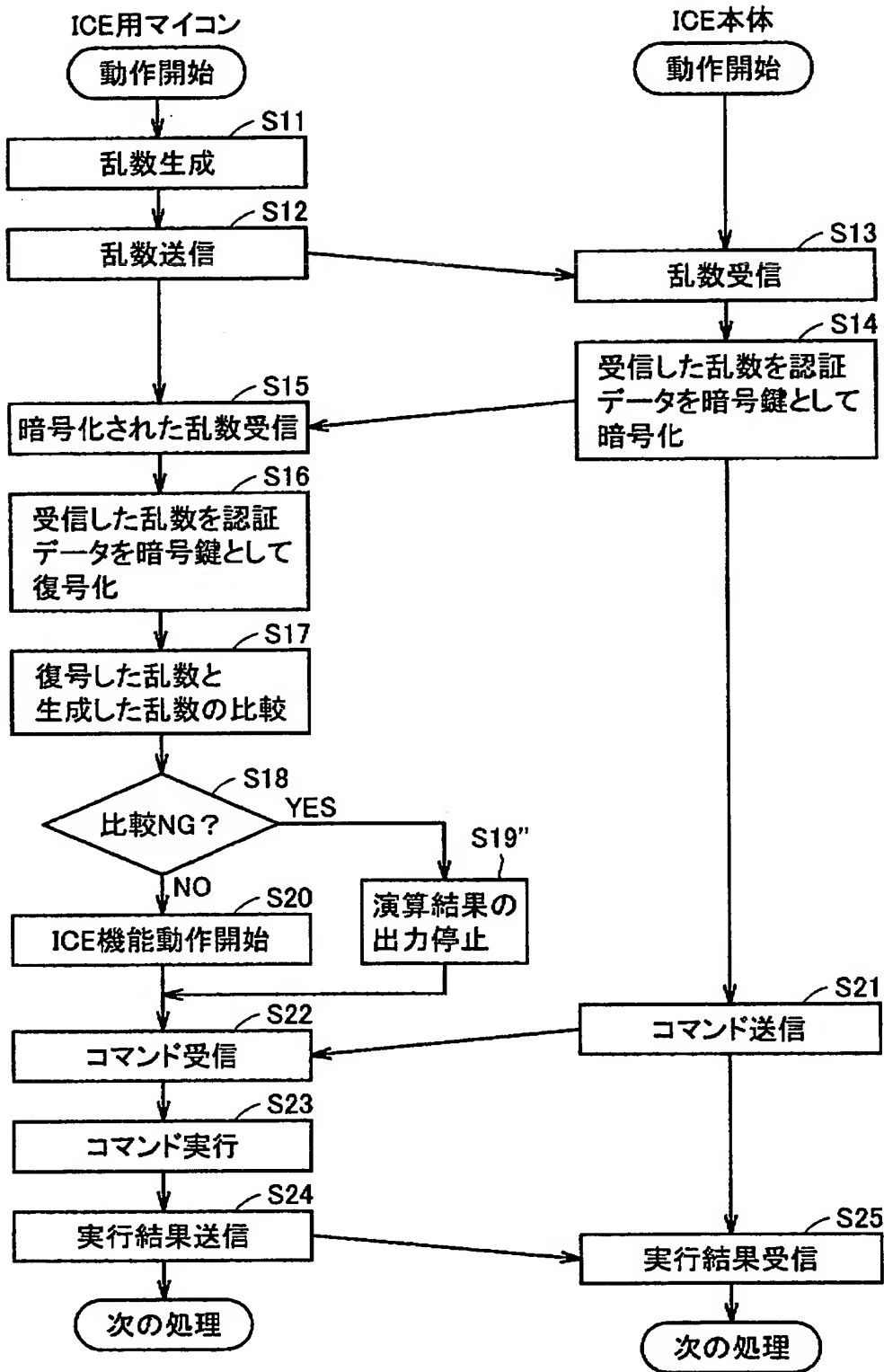
【図 5】



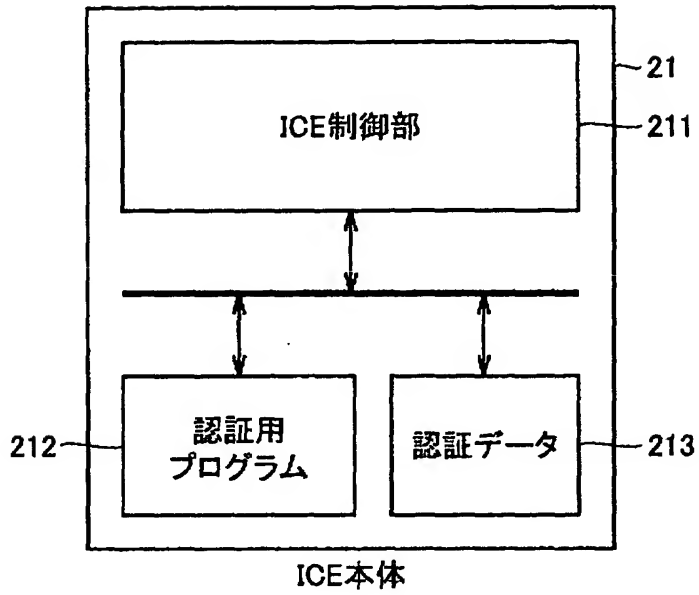
【図 6】



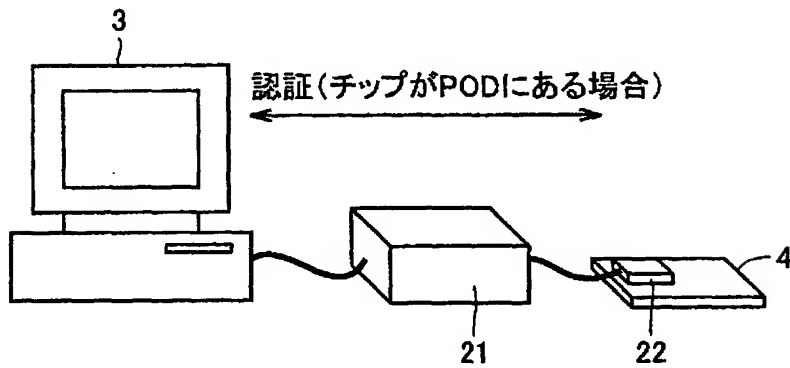
【図 7】



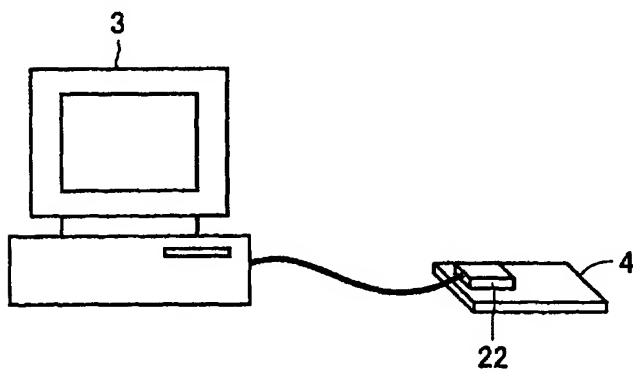
【図 8】



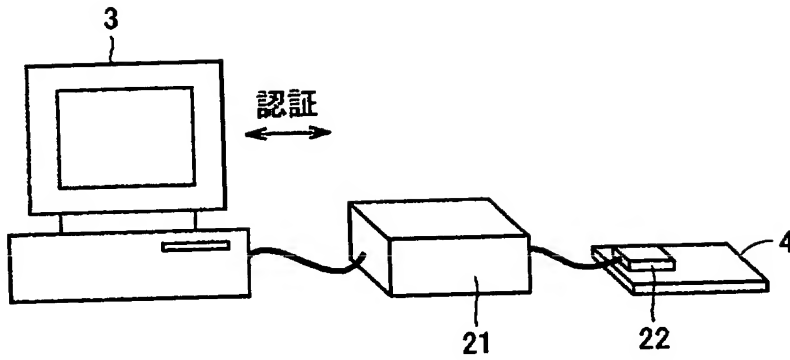
【図 9】



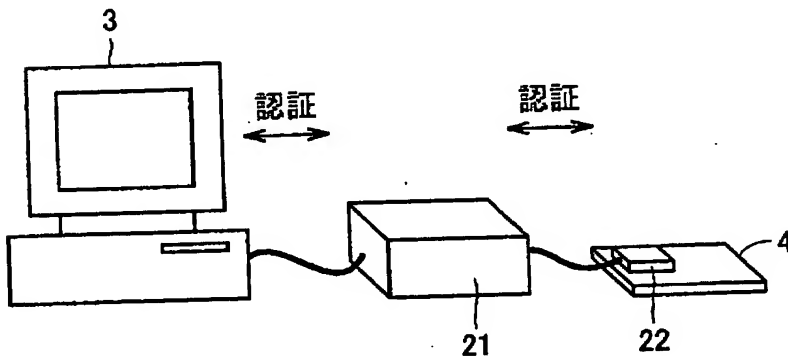
【図 1 0】



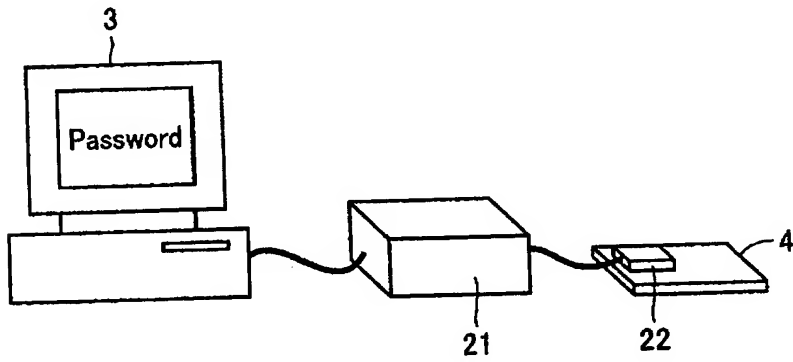
【図 1 1】



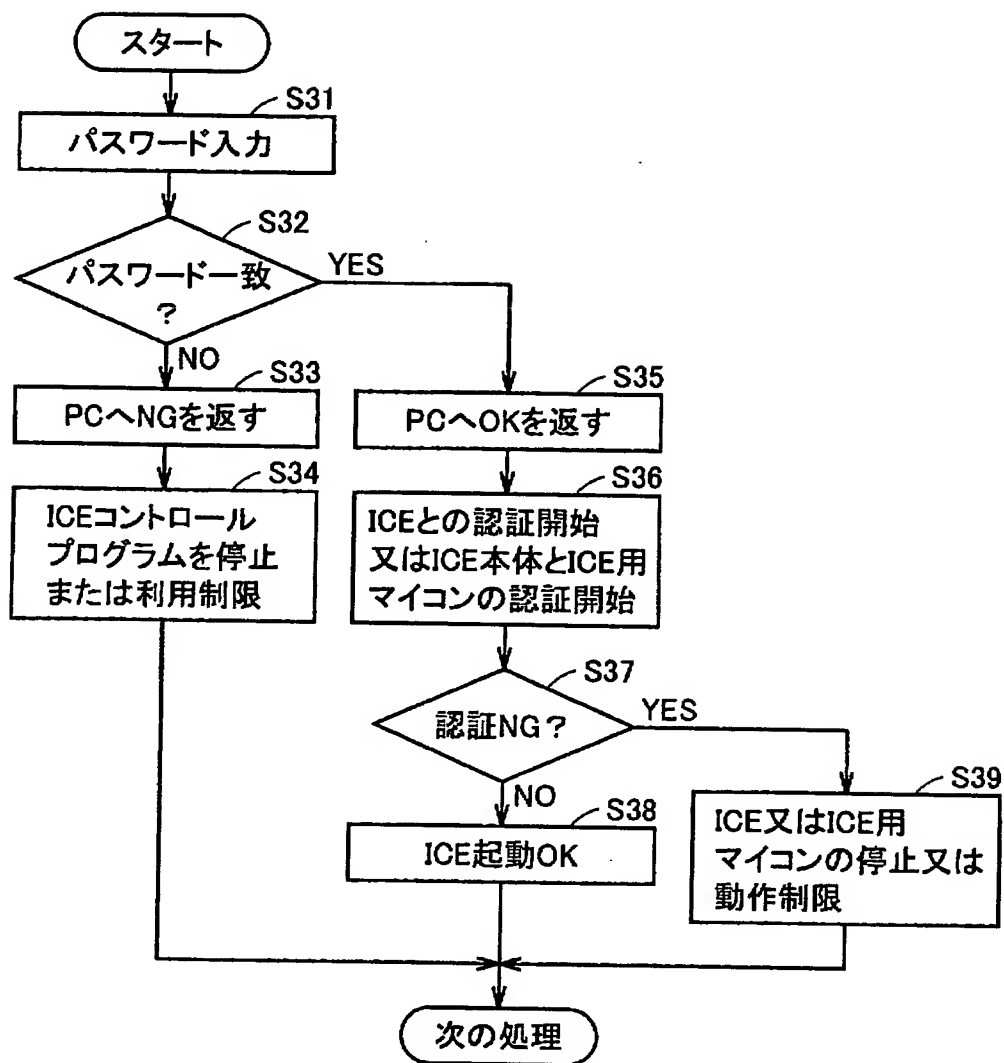
【図 1 2】



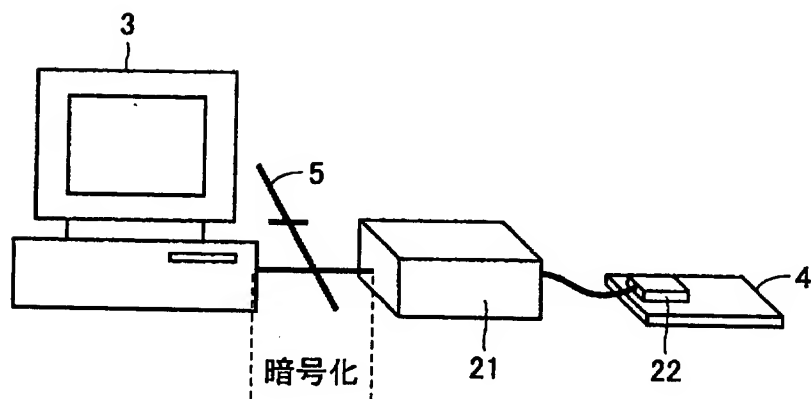
【図 1 3】



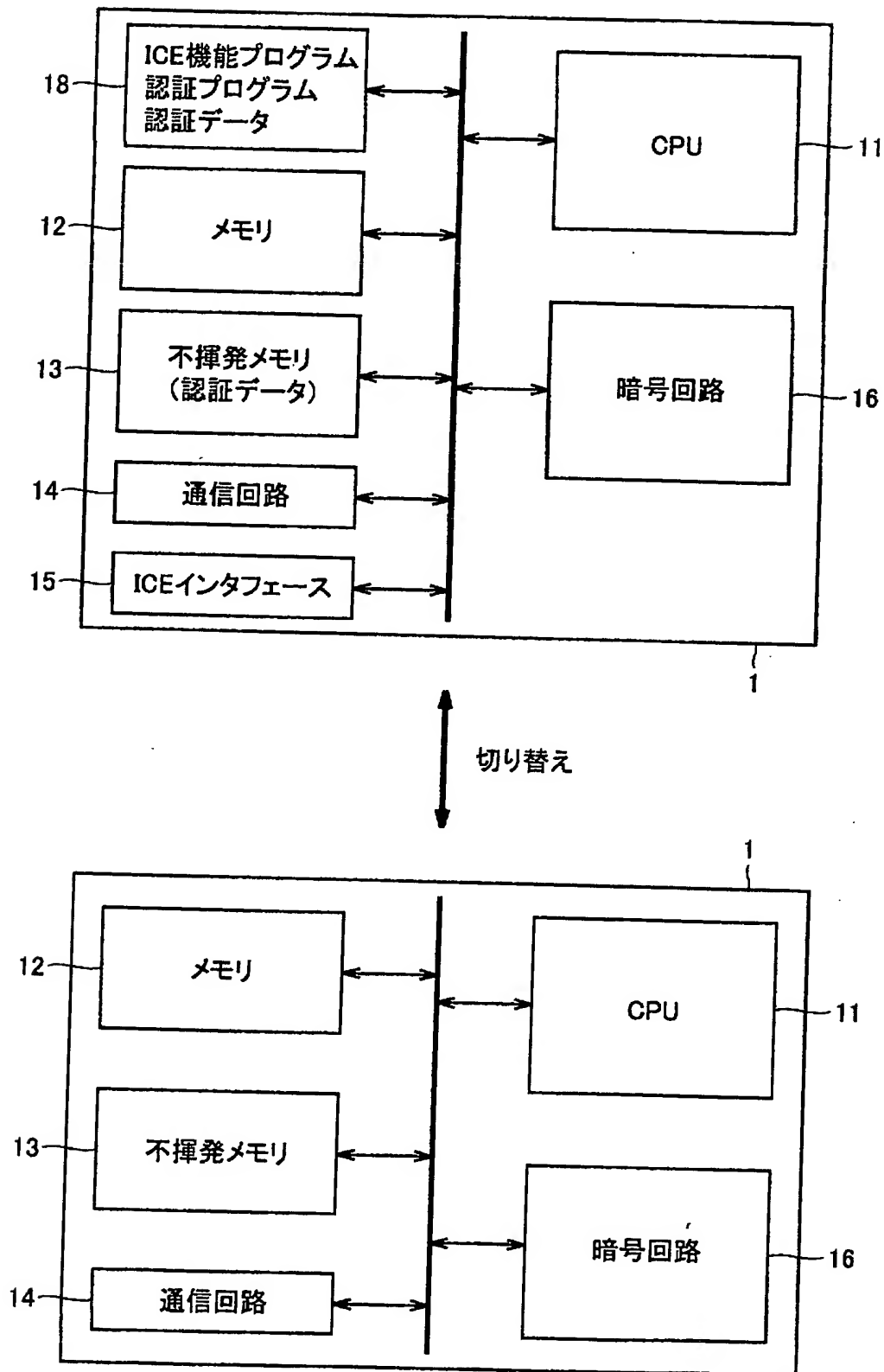
【図 1 4】



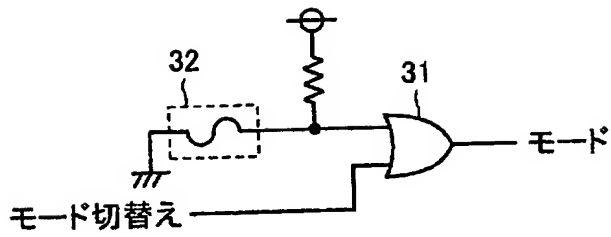
【図 1 5】



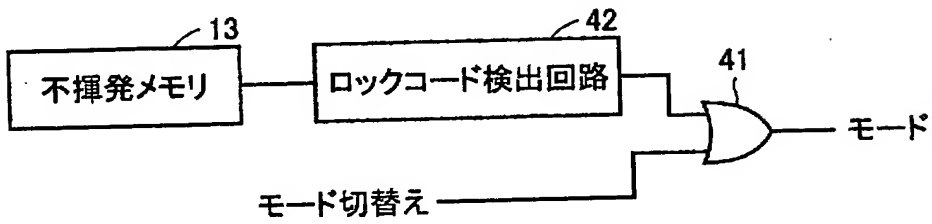
【図16】



【図 1 7】



【図 1 8】



【書類名】 要約書

【要約】

【課題】 使用権限がない者がICE用マイコンとして利用することが不可能な情報セキュリティマイクロコンピュータを提供すること。

【解決手段】 情報セキュリティマイクロコンピュータ1は、情報の暗号化および復号を行なう暗号回路16と、ICE本体の認証を行なう認証用プログラム17と、情報セキュリティマイクロコンピュータ1の全体的な制御を行なうCPU11とを含む。CPU11は、ICE本体の認証が確認されなかった場合には、情報セキュリティマイクロコンピュータ1の少なくとも一部の機能を停止させる。したがって、使用権限がない者が情報セキュリティマイクロコンピュータ1をICE用マイコンとして利用することができなくなり、セキュリティを向上させることが可能となる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日	1990年 8月24日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目2番3号
氏 名	三菱電機株式会社

出 願 人 履 歴 情 報

識別番号 [391024515]

1. 変更年月日	1997年11月26日
[変更理由]	名称変更
住 所	兵庫県伊丹市中央3丁目1番17号
氏 名	三菱電機システムエル・エス・アイ・デザイン株式会社